Abstract

Techniques for single function stage Galois field (GF) computations are described. The new single function stage GF multiplication requires only m-bits per internal logic stage, a savings of m-1 bits per logic stage that do not have to be accounted for as compared with a previous two function stage approach. Also, a common design GF multiplication cell is described that may be suitably used to construct an m-by-m GF multiplication array for the calculation of $GF[2^m] / g[x]$. In addition, these techniques are further described in the context of packed data form computation, VLIW processing, and processing on multiple processing elements in parallel.